COMMONWEALTH OF MASSACHUSETTS

DEPARTMENT OF TELECOMMUNICATIONS AND ENERGY

Investigation by the Department On Its Own Motion, Pursuant To G.L. c. 159 §§ 12 and 16, Into The Collocation Security Policies of Verizon New England D/B/A Verizon Massachusetts	)	**D.T.E. 02-8**

TESTIMONY OF WENDY PERROTT ON BEHALF OF ALLEGIANCE TELECOM OF MASSACHUSETTS, INC.

May 15, 2002

Q. Please state your name, employer, job title and business address for the record.

A. My name is Wendy Perrott. I am a Senior Manager for Colocation Systems in the Network Implementation Department of Allegiance Telecom, Inc., parent company of Allegiance Telecom of Massachusetts, Inc. My business address is 9201 N. Central Expressway, Dallas, Texas75231.

Q. What are your responsibilities as Senior Manager for Colocation Systems?

A. My staff is responsible for submitting all colocation applications to the incumbent local exchange carriers ("ILEC"), verifying connecting facility assignments associated with the applications, monitoring colocation status and readiness, and negotiating and resolving colocation issues with the ILECs, such as badge access and wiring problems. I have been responsible for Allegiance's colocations in the Verizon territories since I joined the company in 1998.

Q. What is the purpose of your testimony?

A. The purpose of my testimony is to respond to the issues raised by Verizon in its Panel testimony and to present Allegiance's position regarding the need for additional colocation security measures in Massachusetts. I find it extremely disconcerting that Verizon is attempting to use the tragic events of September 11, 2001 to limit CLEC colocation options and restrict CLEC access to its central offices. Verizon states at page 18 of its Panel Testimony that "because of recent

[world] events, there is a need to reexamine and strengthen existing security practices and procedures relating to CLEC access to collocated sites." Neither CLECs nor their employees were responsible for the damage done to Verizon's New York network in the wake of the terrorist attacks on the World Trade Center. Indeed, Allegiance's colocation facilities at Verizon's West Street facility were also damaged. As the *Wall Street Journal* article attached to Verizon's Panel Testimony demonstrates, Allegiance and other CLECs pitched in to help Verizon restore service to the many thousands of customers who were taken out of service.

My primary concern is Verizon's proposal to identify certain "critical" central offices in which it would eliminate physical colocation altogether and convert existing physical colocation arrangements to virtual arrangements as well as its proposal to recover all of the costs of any security upgrades it deems necessary from colocators.

Q. Is Allegiance colocated in any Verizon central offices in Massachusetts?

A. Yes. Allegiance has physical colocation arrangements in 35 Verizon central offices. Twelve of the 35 colocations are SCOPE (secured colocation open environment) arrangements and the remainder are traditional caged colocations.

Q. Verizon's witnesses propose that separate and secure space for colocated equipment must be established to reduce security risks and harm to Verizon's network (Verizon Panel Testimony at 23-24). Is Allegiance's

equipment in each of its colocation arrangements located in a segregated and secured area of the Verizon central office?

A. Yes. Verizon confirms on page 10 of its Panel Testimony that caged physical colocation and SCOPE arrangements are located in segregated and secured areas of the central offices.

Q. Does Verizon require Allegiance personnel and vendors to use a separate entrance when accessing the Allegiance colocation arrangements?

A. Yes. In most of the central offices in which Allegiance is colocated, Allegiance personnel and approved vendors use an entrance separate from that used by Verizon personnel.

Q. Do you agree with Verizon that existing security measures are inadequate to protect its network from harm at the central offices where CLECs are colocated?

A. No, I do not. The existing security measures have clearly proven adequate as Verizon itself concedes that "it has not experienced egregious and harmful security violations in Massachusetts" (Verizon Panel Testimony at 21-22). The fact that Verizon has experienced no serious security breaches in Massachusetts either pre- or post- September 11 certainly calls into question the need for additional security measures, especially when Verizon expects CLECs to pay for those measures that will be designed to limit CLEC access to their colocated equipment.

Verizon states that it currently provides 536 traditional "caged" physical colocation arrangements, 385 SCOPE, 27 CCOE and four virtual colocation arrangements (Verizon Panel Testimony at 9-10). As I understand Verizon's testimony, there is no security issue with the virtual colocation arrangements because the CLECs cannot access them and the caged and SCOPE physical colocation arrangements are all provided in separate, secured areas of the central offices (Verizon Panel Testimony at 10-11). Less than half of the 27 CCOE arrangements are in unsecured central office areas and only one of those cannot be relocated due to a lack of available separate and secured space (Verizon Panel Testimony at 34; Verizon Response to Information Request AL-VZ 1-9). Given the current situation, it is not surprising that Verizon has experienced no egregious or harmful security violations in Massachusetts.

Q. Verizon goes to great lengths to describe why its existing security measures "will not prevent some individuals from causing intentional or unintentional damage to Verizon MA's network." For example, it states that it is aware of instances where CLECs have not reported lost access cards or returned cards given to former employees or representatives. Verizon also states that it is aware of CLEC personnel or agents using access cards belonging to others (Verizon Panel Testimony at 18-23). How do you respond?

A. I have to admit that I am somewhat surprised by Verizon's lack of confidence in its security measures given its statement that it has not experienced any harmful security violations in Massachusetts. More importantly, however, Verizon's

proposal to limit colocated CLECs' access to its central offices will not prevent the security breaches it discusses. Verizon has conceded that it is aware of instances where its own employees have not reported lost access cards or have not returned cards given to former employees and representatives as well as of instances where Verizon employees, agents and vendors have used access cards belonging to others (Response to Conversent Information Request 1-14). Because such violations are attributable to Verizon employees, vendors and agents as well as CLEC employees, limiting CLEC access to its central offices will not prevent or eliminate those types of breaches.

Q. Do you think Verizon's concerns about CLECs sabotaging its network – whether inadvertently or intentionally – are well founded?

A. No, I do not. What is missing from Verizon's analysis is any acknowledgement that damage to Verizon's network would by its nature adversely affect interconnected CLECs and their customers. It would not be in any colocated CLEC's best interest to intentionally sabotage Verizon's network or equipment when the very reason the CLEC is colocated in Verizon's central offices is to connect to that network and equipment so that its own customers can complete calls to Verizon customers. I strongly disagree with Verizon's assertion that CLECs have less incentive to guard against unauthorized access to central offices than Verizon employees do. The equipment that CLECs colocate in Verizon's central offices is as much at risk from an unauthorized trespasser as

Verizon's equipment. Accidents, of course, may and will happen, but restricting CLEC access to Verizon's central offices cannot prevent such accidents.

Q. But Verizon states that there is a fundamental difference between its own employees and vendors and CLEC employees and agents. Specifically, Verizon states that its ability to terminate its own employees and vendors creates an incentive for them to follow proper procedures and exercise care and caution when working in the central office. Conversely, according to Verizon, its inability to terminate CLEC employees and agents creates a disincentive for them to follow proper procedures and exercise appropriate care and caution (Verizon Panel Testimony at 31). Do you agree?

A. No, I do not agree and I find Verizon's explanation baffling. It apparently is not Verizon's policy or practice to terminate its own central office technicians or equipment installation technicians for accidentally causing damage within or to Verizon's central offices. Since 1999, Verizon has terminated no employees for accidentally causing damage in a central office (Verizon Response to Information Request AL-VZ-16). Using Verizon's rationale, without fear of termination, Verizon's employees have no more incentive to follow proper procedures and exercise care and caution than CLEC employees. As a result, Verizon's efforts to restrict CLEC access to its central offices to prevent accidents does not seem justified.

Verizon fails to acknowledge that all employers here – Verizon and CLECs – have huge incentives to maintain a properly functioning network so that they can all provide service to their end users. All parties want and need a properly functioning network to conduct

their business. Verizon's failure to acknowledge this shared interest in network security and integrity appears to betray an underlying desire simply not to share that network with competitors, a result I do not believe they can or should achieve in this proceeding.

Q. What do you find most disturbing about Verizon's proposed colocation security plan?

A. The most disturbing aspect of Verizon's security plan is its proposal to eliminate physical colocation entirely at certain "critical" Central Offices for national security reasons and convert any existing physical colocation arrangements at those central offices to virtual colocation arrangements.

Q. How does Verizon define "critical" central offices?

A. Verizon lists a number of very broad criteria that would be used to determine whether a Central Office is "critical." Those criteria include (1) the type of switch or signaling elements housed in a central office with those housing tandem switches, E911 switches and/or STP equipment being deemed "critical"; (2) the presence of critical customers served by a Central Office, including major airports, military installations, government agencies, nuclear power plants, major businesses, public safety agencies, advanced technology companies and other institutions that are involved in national security matters; and (3) the number of access lines and special services circuits served by a Central Office (Verizon Panel Testimony at 39-40).

Q. Has Verizon specified how many of its Central Offices would meet these criteria?

A. No. Significantly, it has not stated how many of the 169 Central Offices in which CLECs are currently colocated would qualify. It has stated only that a "handful" of central offices would meet the criteria (Verizon Panel Testimony at 40). Given the breadth of the criteria that Verizon proposes to use, however, I find it hard to believe that only a "handful" of central offices would meet the criteria. On the contrary, in Attachment 3 to its Panel Testimony, Verizon itself states that "***many*** of Verizon's COs contain emergency 911 (E911) switches and adjunct equipment" (Verizon Panel Testimony, Attachment 3 at 2). In my mind, "many" is not synonymous with "handful" and this example shows just how far reaching Verizon's proposal is. When you add the number of central offices that serve federal, state, county and municipal government agencies, major businesses, advanced technology companies and the other critical customers that Verizon identifies, Verizon would be well on its way to eliminating physical colocation entirely.

Q. You stated earlier that Allegiance has only physical colocations in Massachusetts. Would Allegiance be adversely affected by a requirement that its existing physical colocations be converted to virtual or that it be limited to virtual colocation as it expands its network footprint?

A. Yes. Although Allegiance has no virtual colocations in Massachusetts, it has had very poor experiences with virtual builds in Verizon territory in New York, New Jersey and Pennsylvania, and this has negatively impacted our ability to service existing customers and turn up new customers. Having no access to our colocated equipment means that we are completely dependent upon Verizon and its technicians' schedules to do any necessary maintenance and repairs. We have experienced poor response time from Verizon for DS3 maintenance and delivery, difficulty ordering and installing POTS lines for remote diagnostic testing of integrated digital loop carriers and poor connecting facility assignment ("CFA") documentation.

We have also experienced problems when we have tried to add to our virtual colocation arrangements. Verizon, of course, cannot guarantee that there will be contiguous space available and the space designated for our new equipment may be across the building or across the aisle.

Finally, Allegiance has had negative experiences with establishing new virtual colocation arrangements in Verizon central offices in other states. Verizon has a limited list of vendors approved to do installation work for CLECs in central offices. Because there are so few from which to choose, the approved vendors were consistently booked doing virtual work for numerous CLECs. Allegiance project managers were limited in the number of access trips they could make to check on the progress of virtual builds and so were forced to rely on the vendors for progress reports, which were often inaccurate. The vendors' work was not

always as good as it should have been and several installations had to be rebuilt or fixed at the last minute. Before a virtual colocation is turned up and the CFA activated in Verizon's databases, a final inspection has to be done by the Verizon Central Office manager and a Verizon appointed inspector. The approved inspectors always had full schedules and turn ups were frequently delayed by weeks because an inspector was not available. To the extent that CLECs are unnecessarily delayed in turning up colocations, the clear beneficiary is Verizon. Without access to the central office and the unbundled network elements they need to provide service, facilities-based CLECs are unable to timely implement customer orders and start generating revenue.

As a result of these experiences, Allegiance has not done a new virtual colocation arrangement in a central office anywhere in the Verizon region since March 2000. After Verizon informed Allegiance in September 1998 that there was not enough space to install an IDLC in a physical colocation arrangement in the Lexington central office, Allegiance delayed offering service to customers served by that office until SCOPE became available, rather than deploy a virtual arrangement.

Q. Please comment on Verizon's proposal that CLECs pay the full cost of any new security measures implemented, including the costs of converting existing physical colocation arrangements to virtual.

A. Requiring CLECs to foot the entire bill would be unacceptable. Allegiance paid considerably higher nonrecurring charges for its physical colocation arrangements

in Massachusetts than it would have paid for virtual arrangements. Should the Department agree with Verizon that virtual colocation should be required in certain "critical" central offices, which it should not, CLECs should not be required to pay any of the costs for converting physical colocation arrangements to virtual. In addition, Verizon should be required to refund the difference between the nonrecurring charges Allegiance has already paid for physical colocation and what it would have paid for virtual colocation because Allegiance will be getting substantially less than it paid for in a virtual colocation arrangement to which it has no access. Under no circumstances should CLECs be required to pay nonrecurring charges a second time for rearrangements done at Verizon's behest for security concerns that have not been shown to be valid.

To the extent that Verizon decides to upgrade its existing security systems by providing CLECs escorted access to their colocation arrangements and adding electronic card reader access systems or closed circuit television cameras in areas where CLECs are colocated that are not already segregated and secured, Verizon should at a minimum be required to share those costs because it will also share the benefits.

Q. To your knowledge, has any other incumbent local exchange carrier proposed to eliminate physical colocation or to recover the costs of upgrading its central office security systems solely from colocating CLECs?

A. Allegiance is colocated in the central offices of all of the Regional Bell Operating Companies. No other carrier has proposed such drastic and anti-competitive measures.

Q. Does this conclude your testimony?

A. Yes.